Unrestricted Access to Mainframe Data Sets and Resources

Effective: June 21, 2000
Revised: May 25, 2000
Owner: Bart Grant

Purpose

To define the circumstances under which logon IDs, with unrestricted accesses to the State's Mainframe computer resources and data, may be used and to specifically allow ITS technical personnel necessary access to system data and resources when emergency conditions require immediate action.

Scope

This policy applies to all employees with ACF2 NON-CNCL, READALL or MAINTENANCE access to the State's mainframe computer resources and data.

Background

NON-CNCL, READALL, and MAINTENANCE (MAINT) are attributes on ACF2 Logon IDs which provide unlimited read and/or write access to mainframe data and resources. These attributes on an ACF2 logon ID allow tasks using the logon ID to access mainframe resources even though ACF2 would normally deny the access. The NON-CNCL privilege allows read and write access to data sets and resources while preserving audit trails. READALL allows read only access to data sets, while preserving audit trails. The MAINT privilege, in conjunction with a valid MAINT record, bypasses ACF2 rule validation and creates no SMF logging records.

Some ITS personnel (System Programmers, Database Administrators, Space Management) have been provided with NON-CNCL and READALL access in order to respond to emergency outages. These functions must be supported and monitored. ITS customers and auditors have legitimate concerns about access allowed by these attributes and must be assured that each of these accesses are legitimate and necessary.

POLICY

All access to mainframe data and resources will be authorized by the custodian of that resource. The data or resource custodian will provide access to authorized people through ACF2 data set or resource rules. ACF2 data set and resource rules will be maintained either by authorized agency security administrators or by ITS Data Security at the request of an authorized agency security administrator.

NON-CNCL and READALL Access

ITS personnel will use their primary ACF2 logon ID (without the NON-CNCL or READALL privileges) for routine purposes. If any access to data or resources is needed, but not allowed to their primary logon ID by ACF2 Rules, the ITS personnel will contact the owner or custodian of the data set or resource and request that they provide access through rules. The owner or custodian of the data set or resource will use existing forms and notification methods to inform their Agency Security Personnel or ITS Data Security that the requested access has been authorized. (Temporary or permanent access may be granted.)

ITS Data Security Staff will be available during regular work hours, or on-call during off shift hours, weekends, and holidays to assist with rule changes.

ITS Technical personnel will use logon IDs with NON-CNCL or READALL privileges only when a service outage exists and critical systems or applications depend upon them having immediate access to data or resources that are not currently allowed by rules.

Whenever a data set or resource is accessed with a NON-CNCL or READALL logon ID, an ACF2 logging entry will be created. The ACF2 log report is used to notify the custodian agency's Security Administrator, the manager of the ACF2 logon ID's owner, and ITS Data Security. Agency security administrators, auditors, or ITS Data Security will make a follow-up contact with the person making the NON-CNCL or READALL access to determine if future access should be allowed by the ACF2 rules. The ITS person making the NON-CNCL or READALL access will answer the questions of Security personnel or auditors concerning this access.

NON-CNCL and READALL privileges may be requested for ITS employees only by their manager.

Maintenance Access

MAINT records will be created for STARTED Task logon IDs when needed. ITS technical personnel will be given the MAINT privilege only for documented system maintenance purposes (disk compression, archiving, etc.). Maintenance records will be documented by ITS/Security and made available for auditors and agency security administrators to review periodically.

MAINTENANCE privilege will be authorized for ITS employees by their manager.